readytech

Open Windows Software Security Processes

July 2022

Table of Contents

1. Introduction

Open Windows software solutions do not replace people, they turn administrators and business system owners back into managers, freeing them of manual administration tasks and allowing them to focus on the business' real needs.

Our mission is to empower users of our technologies to make positive systemic change in their organisations, to bring bottom line cost savings and process improvement.

Pioneers in the procurement and contracting technology space, we will continue to build software and deliver solutions that provide greater value to organisations, enhancing and strengthening relationships both within and outside the business.

Making sure your data is secure and protecting it is one of ReadyTech's most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

2. Security and Compliance

ReadyTech has established an industry-leading security program, dedicated to ensuring customers have the highest confidence in our custodianship of their data. Our Information Security Management System (ISMS) is aligned to the ISO 27000 standards and is regularly audited and assessed by third parties.

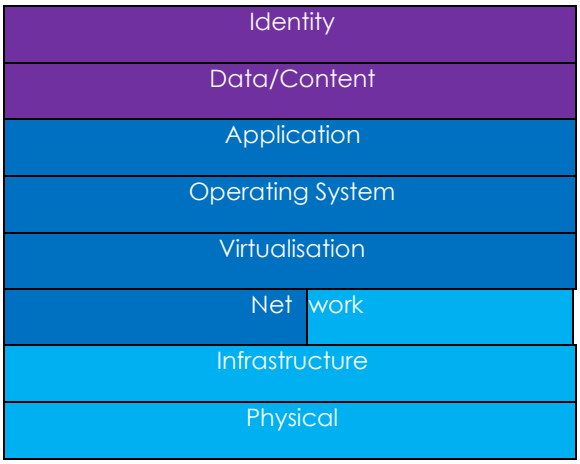
Our ISO 27001:2013 certificate is available on the JAS-ANZ register:
https://register.jas-anz.org/certified-organisations

3. Shared Security Responsibility Model

ReadyTech strives to protect the confidentiality, integrity and availability of all critical information and stored customer data.

While we manage security *of* the application, security *in* the application is the responsibility of the customer. Open Windows Software is provided as software-as-a-service, i.e., a fully functioning modern web application. ReadyTech is responsible for procuring, configuring, monitoring and maintaining all aspects of the computing environment, from the servers to the application. ReadyTech utilises Microsoft Azure, which is the world leading provider of cloud infrastructure. Microsoft Azure physical and technical security practices are outlined in its whitepaper at https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

The customer is responsible for managing the access of their authorised users, password policies and configuring roles and permissions within the application itself.



	Customer Responsibility	Security **in** the application
	ReadyTech Responsibility	Security **of** the application
	Azure Responsibility	Security **of** the cloud

3.1 Infrastructure

Open Windows Software is hosted in the public cloud with Microsoft Azure. Azure provides state-of-the-art data centers and a world-leading compliance program. Microsoft operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which Open Windows Software operates. Azure manages the network devices, but ReadyTech is responsible for secure network configuration.

3.2 Data Sovereignty

Open Windows uses the Azure Australia SouthEast region for primary data storage, secondary storage locations (for replication services) are in the Australia East region. This ensures data is only stored and processed within Australia.

3.3 Data Ownership

The customer always owns their data. ReadyTech collects and processes data on behalf of the customer as required to provide and support the platform, as further detailed in the Privacy Policy: readytech.io/privacy

4. Personnel Security

All ReadyTech staff undergo screening checks before employment including reference, qualification and police checks. Security awareness training is provided at initiation and continuously throughout the year. Staff with privileged access to systems or data receive additional job-specific training on privacy and security. Personnel requiring access to production systems or customer data are required to have undergone appropriate security clearances.

ReadyTech has appointed a Chief Information Security Officer who is responsible for the performance of the ISMS. All staff have security responsibilities assigned as part of their roles. Open Windows has also identified a Quality and Information Security Officer (QISO) for the governance and management of the Integrated Quality Management and Information Security Management Systems (IMS) of Open Windows Software.

5. Identity and Access Management

Open Windows Software is accessed via a customer choice for authentication. Forms Authentication allows for a customised password policy to be defined by the customer, all usernames and passwords are stored within the customer's tenant, and passwords are hashed using SHA256.

Alternatively, customers can integrate their SSO solutions with the following native plugin options available:

- AzureAD (OpenID connect)
- ADFS (WS Federation)
- Okta (OpenID connect)

Access for ReadyTech staff to the application and infrastructure is provided on a least necessary privilege basis, with technical controls limiting access to approved staff, authenticated with MFA in the central authentication system. All access is authorised before setup and regularly reviewed.

6. Standard Operating Environments

All hosted/cloud servers are provisioned using standard container configurations within Microsoft Azure. They are hardened and configured with Automatic Updates and mandatory real time protection all configured by Group Policy. Environments are joined to the AzureAD Domain Service with access controls enabled with permissions on a least privileged basis. During provisioning, the appliance is added to the Nagios monitoring solution for real time service and event monitoring.

7. Patch Management

Cloud server environments are provisioned using standard container templates with Automatic Updates and Automated Scans configured on provisioning.

Vulnerabilities in application libraries or frameworks are identified from 3rd party news sources and patched in standard software development workflows, with emergency release if required.

8. Software Development

The Development process is conducted utilising Agile methodologies using a secure development standard. All code must pass unit tests, peer review and QA testing in a dedicated QA environment before it is passed for release to customer non-production and production environments.

9. Database Systems

Each customer (tenant) uses a logically isolated database. All customers retain their own individual database for the storage of contract, sourcing, project, supplier, workflow, categories, master data (process, custom fields, custom forms) data.

The tenant databases are portable, if desired/required, a customer database can be re-deployed to an alternate or dedicated database cluster. This is not offered as standard and additional costs will apply.

The logical network design ensures all connectivity points are maintained using best practice design in securing communication channels. This includes encryption of communication points, or protection of services behind firewalls. Firewall rules or NAT rules are applied to only the available/applicable services to deliver the requirements of each service.

10. Network Security

Azure Network Security Groups are used to expose only least necessary network ports to the public internet. Each Azure host has Windows Firewall configured to expose necessary services only.

Administrative access is limited to only networks/devices where management connections would be expected to originate.

ReadyTech corporate offices are protected by a firewall.

11. Cryptography

All disks within the Microsoft Azure platform are encrypted at rest with Storage Service Encryption (SSE) using platform managed keys. SSE is encrypted using the AES-256 algorithm.

Transport Layer Security (TLS) is used for all public network connections using TLS V1.2 or above with TLS V1.3 supported. ReadyTech audit TLS compliance via a weekly automated scan.

12. Logging and Monitoring

Logging for hosted servers is centrally managed using Nagios with alerting that goes to the Operations team.

Network Devices (Routers, Switches, Firewalls Logs are reviewed by the QISO and actioned as necessary.

13. Backup Management

All cloud-based servers are backed up nightly utilising Azure Recovery Services, configured with Geo Redundancy, and multiple replica copies for maximum protection. The frequency of the backups is tailored to suit both Open Windows Software operational requirements, and customers data held within Open Windows Software. Transaction logging allows for point in time recovery within 1 minute, site to site replication services enables near real time recovery point objectives.

14. Data Retention

Data is retained within the system for the life of the contract. At contract termination, data is returned to the customer and permanently destroyed according to standard operating procedures. Data will be made available in standard, documented formats via the platform as a "Transition Out" service.

Database backups are retained within retention policies and deleted by automated lifecycle policies.

15. Business Continuity

The concepts of business continuity and disaster recovery are integrated into our design and architecture of highly available systems in the public cloud. Failure is routinely expected, planned for, tested and managed with automated systems and redundancy.

Resilience and scalability are addressed on Azure through:

- Running full recovery mode on databases to allow for point in time restoration
- Application layer availability and scalability managed through Azure.

Data and assets are versioned, backed up and monitored.

16. Incident Management

ReadyTech has documented Incident Response, Business Continuity, Disaster Recovery, Security and Data Breach Response, and Crisis Management Plans that are tested at least annually.

Customers will be notified in accordance with our Incident response or Data Breach response plans in the case of an incident, the timing of which is outlined in the relevant plans and is based on the severity and urgency. The nominated role at ReadyTech will continue to communicate with the customer on the specified schedule at a minimum until the issue is resolved. In general, ReadyTech takes the approach of informing the customer as soon as is practical in all cases.

17. Third Party Supplier Management

ReadyTech relies on sub-service organisations, such as Azure, to run its business efficiently. We evaluate and qualify our vendors with a risk-based approach and documented standards which include security, technical and financial assessments. ReadyTech ensures our security posture is maintained through legal agreements and regular security compliance review of these arrangements.

18. Contacts

ReadyTech is continually striving to keep our systems secure. If you become aware of any security issue or have any further queries regarding this document, please contact the security team directly at security@readytech.io.

19. Classification

This document is **Public**; it is approved for public release.

20. Document Management

Version	Date	Initials	Description
1.0	20/07/2022	RD/SG	Prepared for distribution